Hidden Lynx – Professional Hackers for Hire

Created: 17 Sep 2013 13:00:01 GMT

Symantec Security Response Symantec Employee
+4 4 Votes
Login to vote

Tweet

For the past few years, reports have continued to emerge detailing the activities of actors behind various targeted attacks or Advanced Persistent Threats (APTs). Here at Symantec Security Response, we've been keeping our eyes on a group that we believe are among the best of breed. We've given them the name of Hidden Lynx—after a string that was found in the command and control server communications. This group has a hunger and drive that surpass other well-known groups such as APT1/Comment Crew. Key characteristics of this group are:

- technical prowess
- agility
- organized
- sheer resourcefulness
- patience

These attributes are shown by the relentless campaigns waged against multiple concurrent targets over a sustained period of time. They are the pioneers of the "watering hole" technique used to ambush targets, they have early access to zero-day vulnerabilities, and they have the tenacity and patience of an intelligent hunter to compromise the supply chain to get at the true target. These supply chain attacks are carried out by infecting computers at a supplier of an intended target and then waiting for the infected computers to be installed and call home, clearly these are cool calculated actions rather than impulsive forays of amateurs.

This group doesn't just limit itself to a handful of targets; instead it targets hundreds of different organizations in many different regions, even concurrently. Given the breadth and number of targets and regions involved, we infer that this group is most likely a professional hacker-for-hire operation that are contracted by clients to provide information. They steal on demand, whatever their clients are interested in, hence the wide variety and range of targets.

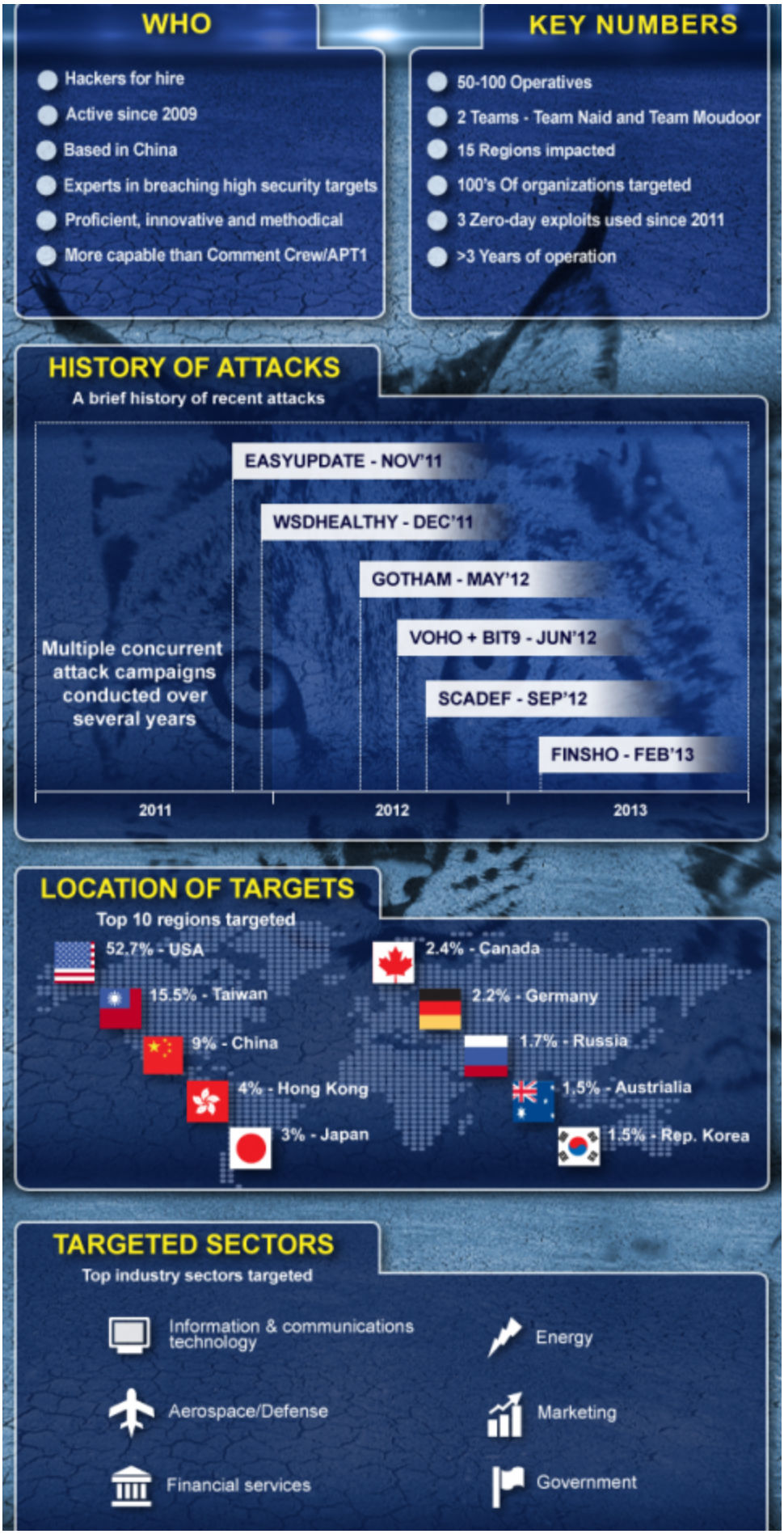
We also believe that to carry out attacks of this scale, the group must have considerable hacking expertise at its disposal, perhaps 50 to 100 operatives are employed and organized into at least two distinct teams both tasked with carrying out different activities using different tools and techniques. These types of attacks require time and effort to carry out, some of the campaigns require research and intelligence gathering before any successful attacks can be mounted.

At the front line of this group is a team that uses disposable tools along with basic but effective techniques to attack many different targets. They may also act as intelligence collectors too. This team we call Team Moudoor after the name of the Trojan that they use. Moudoor is a back door Trojan that the team uses liberally without worry about discovery by security firms. The other team acts like a special operations unit, elite personnel used to crack the most valuable or toughest targets. The elite team uses a Trojan named Naid and are therefore referred to as Team Naid. Unlike Moudoor, the Naid Trojan is used sparingly and with care to avoid detection and capture, like a secret weapon that is only used when failure is not an option.

Since 2011, we have observed at least six significant campaigns by this group. The most notable of these campaigns is the VOHO attack campaign of June, 2012. What was particularly interesting about this attack was the use of the watering hole attack technique and the compromise of Bit9's trusted file signing infrastructure. The VOHO campaign was ultimately targeting US defense contractors whose systems were protected by Bit9's trust-based protection software but when the Hidden Lynx attackers' progress was blocked by this obstacle, they reconsidered their options and found that the best way around the protection was to compromise the heart of the protection system itself and subvert it for their own purpose. This is exactly what they did when they diverted their attention to Bit9 and breached their systems. Once breached, the attackers quickly found their way into the file signing infrastructure that was the foundation of the Bit9 protection model, they then used this system to sign a number of malware files and then these files were used in turn to compromise the true intended targets.

For those interested in more in-depth information, we have published a whitepaper that describes the group and the attack campaigns carried out by them.

We have also put together an infographic that summarizes the key information about this prolific Hidden Lynx group.


WHO
Hackers for hire
Active since 2009
Based in China
Experts in breaching high security targets
Proficient, innovative and methodical
More capable than Comment Crew/APT1
KEY NUMBERS
50-100 Operatives
2 Teams - Team Naid and Team Moudoor
15 Regions impacted
100's Of organizations targeted
3 Zero-day exploits used since 2011
>3 Years of operation
HISTORY OF ATTACKS
A brief history of recent attacks
Multiple concurrent attack campaigns conducted over several years
EASYUPDATE - NOV'11
WSDHEALTHY - DEC'11
GOTHAM - MAY'12
VOHO + BIT9 - JUN'12
SCADEF - SEP'12
FINSHO - FEB'13
2011
2012
2013
LOCATION OF TARGETS
Top 10 regions targeted
52.7% - USA
15.5% - Taiwan
9% - China
4% - Hong Kong
3% - Japan
2.4% - Canada
2.2% - Germany
1.7% - Russia
1.5% - Austrialia
1.5% - Rep. Korea
TARGETED SECTORS
Top industry sectors targeted
Information & communications technology
Energy
Aerospace/Defense
Marketing
Financial services
Government

Blog Entry Filed Under: